

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)	
)	
Implementation of the)	CC Docket No. 96-115
Telecommunications Act of 1996:)	
)	
Telecommunications Carriers' Use of)	
Customer Proprietary Network Information)	
And Other Customer Information;)	
)	
Implementation of the Non-Accounting)	CC Docket No. 96-149
Safeguards of Section 271 and 272 of the)	
Communications Act of 1934, As Amended)	
)	
2000 Biennial Regulatory Review <input type="checkbox"/>)	CC Docket No. 00-257
Review of Policies and Rules Concerning)	
Unauthorized Changes of Consumers')	
Long Distance Carriers)	

COMMENTS OF AT&T WIRELESS SERVICES, INC.

AT&T Wireless Services, Inc. ("AWS") hereby submits its comments in response to the Commission's *Third Further Notice* in the above-captioned proceeding.^{1/}

INTRODUCTION AND SUMMARY

The Commission asks parties to refresh the record on certain aspects of its customer network proprietary information ("CPNI") rules in light of recent industry consolidation and in response to the Nation's heightened security concerns. Specifically, the Commission seeks further comment on the FBI's 1997 proposal to bar carriers from storing CPNI in foreign

^{1/} *Implementation of the Telecommunications Act of 1996; Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, As Amended, 2000 Biennial Regulatory Review – Review of Policies and Rules Concerning Unauthorized Changes of Consumers' Long Distance Carriers*, CC Docket Nos. 96-115, 96-149, 00-257, Third Report and Order and Third Further Notice of Proposed Rulemaking, 17 FCC Rcd 14860 (2002) ("*Third Further Notice*").

countries and from allowing access to CPNI from foreign locations.^{2/} The Commission also asks whether it should permit CPNI to be shared with an acquiring company when a carrier sells its assets or goes out of business.^{3/}

If the Commission chooses to adopt foreign storage or access restrictions, AWS urges it to clarify that the CPNI of wireless customers obtained when the customers are roaming overseas is not included within the scope of the rules. If AWS' foreign roaming partners are not able to generate and store information about the origination, destination, and duration of calls made on their networks, or to access data sufficient to verify that AWS is the valid home carrier of the roamer, they will not be able to provide, or bill for, service. This would preclude international roaming, which obviously is not a positive result for either U.S. consumers or U.S. competition.

In addition, the Commission should not restrict the sharing of CPNI in the context of business transfers because doing so could prevent the new carrier from providing service to the acquired customers. This clearly would undermine the Commission's and carriers' joint goal of ensuring uninterrupted coverage notwithstanding changes in the ownership or control of the service provider. In addition, the Commission should not require carriers immediately to reissue "opt-out" notices to newly acquired customers because, in any case, all carriers are required to do that every two years.

^{2/} *Third Further Notice* ¶ 146.

^{3/} *Id.* ¶ 146.

I. THE FCC SHOULD CLARIFY THAT THE CPNI OF DOMESTIC WIRELESS CUSTOMERS ROAMING OVERSEAS DOES NOT FALL WITHIN THE SCOPE OF THE FBI'S PROPOSED FOREIGN-STORAGE OR ACCESS RESTRICTIONS

The Commission asks for comment on the FBI's 1997 request that the Commission regulate the foreign storage of, and foreign-based access to, CPNI of U.S. customers that use domestic telecommunications services.^{4/} The FBI's letter proposes that the CPNI of domestic customers be stored exclusively in the United States and that access to CPNI from foreign locations be prohibited. In the alternative, the FBI argues that foreign storage and direct foreign access to domestic CPNI should be permitted only upon informed written customer approval.^{5/} The FBI also asks that, to the extent CPNI is stored overseas, the Commission require carriers to keep a copy of the CPNI records within the United States.^{6/}

Apparently recognizing that U.S. carriers have no control over their foreign counterparts' use of CPNI when customers actually obtain telecommunications services in the foreign location, the FBI limited the scope and application of its letter to "customers who only subscribe to domestic telecommunications services."^{7/} This exclusion appears to encompass U.S.-based wireless customers that use foreign networks to place and receive calls when traveling. For the reasons discussed below, AWS urges the Commission to make this wireless roaming exemption explicit in any CPNI foreign storage rules it may adopt.

^{4/} *Third Further Notice* ¶ 144.

^{5/} See Letter from John F. Lewis, Jr., Asst. Dir. in Charge, Federal Bureau of Investigation, to William F. Canton, Acting Secretary, Federal Communications Commission 9 (dated July 8, 1997) (on file with the Commission in CC Docket No. 96-115) ("*FBI Letter*").

^{6/} *Id.* at 5 n.8.

^{7/} *Id.* at 1 n.1.

Although the FBI letter mentions “mobile phones” in several places, the FBI’s concern plainly was directed to the foreign storage of call records of customers who place and receive calls within the United States; not to mobile phone use overseas on a foreign carrier’s network.^{8/} Some basic facts about roaming demonstrate why a roaming exemption from foreign storage or access restrictions is necessary. When an AWS customer roams on a foreign network, the foreign carrier essentially steps into AWS’ shoes as the service provider. To complete calls, the roamed-on carrier clearly must know where the customer is calling and from where the call is placed. In addition, to bill for the service, the foreign carrier must be able to verify whether the customer is served by AWS in the United States, as well as the duration, origin, and destination of each call placed and received in the foreign country. If AWS’ foreign roaming partners were not able to generate and store this CPNI, AWS’ customers would not be able to roam internationally. This would not be in the best interest of consumers, who obviously sign up for international roaming service precisely because they want to roam internationally.

For these same reasons, wireless carriers should not be required to obtain prior written consent from their customers to store abroad or access the CPNI that is generated while the customers are roaming in other countries.^{9/} When AWS’ customers subscribe to an international roaming service and use their handsets in foreign locations, they are fully aware that the foreign carrier would not be able to provide them service unless it can collect and store information about the calls they make and receive. Thus, in the event that AWS was unable to obtain prior

^{8/} *Id.* at 8, n.17 (arguing that direct access to home or mobile phone activity records from abroad could compromise security and safety).

^{9/} The FBI proposes that carriers obtain written consent from the customer and suggests that the carrier ask the customer to write “I, [customer], hereby authorize Carrier X to store my CPNI in [country Y] and/or permit direct foreign electronic access to my CPNI from [country Y].” *See FBI Letter* at 9-10 n.20.

written consent pursuant to the FBI's "opt-in" proposal before its customer departed on his or her trip, the customer would not be able to roam. Likewise, carriers should not have to obtain consent in order to provide services to, or on behalf of, customers from overseas locations. It would be practically impossible to obtain such consent if a subscriber's call to customer service, for example, were routed to a customer care representative located outside the United States.

AWS does not object to maintaining copies of foreign-generated CPNI within the United States, but it cannot guarantee that this information will be available immediately in every case. While, for its own billing purposes, AWS would like to dictate how quickly its foreign roaming partners must transmit call records back to AWS, the fact is that AWS has little control over this process. From some countries, the turn-around time is a matter of days, and sometimes even hours, but other roaming partners, particularly those located in smaller or underdeveloped countries, often take weeks or months to route the information back to AWS.^{10/} As it does today, however, AWS will continue to work closely with law enforcement officials to comply with their requests for customer information, pursuant to lawful authority, and to deliver this information as promptly as possible.

II. CARRIERS SHOULD BE PERMITTED TO SHARE CPNI FREELY AS PART OF A BUSINESS TRANSFER

Carriers should be able to use and disclose CPNI when they sell their assets or go out of business. As a threshold matter, it is not clear how any purchase/sale transactions involving FCC-regulated carriers could occur absent the transfer of CPNI. Without basic information, such as the type of services to which customers subscribe, the new carrier would not be able to

^{10/} For example, the CPNI collected by AWS' affiliates in the Caribbean is sent to AWS' billing center in Atlanta several times per day. For other foreign carriers, it can take up to three months for the information to be returned to AWS for billing and collection purposes.

provide service to the acquired customers and would not be able to honor its assumed contractual obligations. Not only would such a rule severely burden telecommunications mergers and acquisitions, it would not serve customers, who presumably have an interest in retaining seamless service throughout a sale or bankruptcy.

Nor is there any reason why an exiting carrier should be required to provide advance notice to, and obtain consent from, customers regarding the transfer of their CPNI to the new carrier. Adding a new and separate requirement for CPNI on top of the Commission's existing verification (slamming) rules would be unduly cumbersome and ultimately confusing for consumers.^{11/} This additional requirement would be especially burdensome in the wireless context because the Commission previously has determined that the verification process is not necessary to protect CMRS customers.^{12/}

More fundamentally, the Commission's goal of protecting consumer privacy would not be furthered by conditioning the sharing of CPNI between selling and purchasing carriers on advance notice. The use and disclosure of CPNI during a business transfer cannot be considered to be an unexpected use of a customer's personal information, particularly when carriers place their customers on notice that CPNI may be used or disclosed for this purpose. For example, the AWS subscriber agreement notifies customers that their information may be disclosed as part of any merger, acquisition, or sale of the company, as well as in the unlikely event of insolvency, bankruptcy or receivership. In addition, AWS maintains a "Business Transfer" clause in its

^{11/} *Third Further Notice* ¶ 146; *see also* 47 C.F.R. § 64.1120(e).

^{12/} *See* 47 C.F.R. § 64.1120(a)(3); *see also Implementation of the Subscriber Carrier Selection Changes Provisions of the Telecommunications Act of 1996: Policies and Rules Concerning Unauthorized Changes of Consumers' Long Distance Carriers*, CC Docket No. 94-129, Second Report and Order and Further Notice of Proposed Rulemaking, 14 FCC Rcd 1508 ¶ 85 (1998).

privacy policy to notify customers of such disclosures.^{13/} Given both the contractual notice and the disclosures made in AWS' privacy policy, there is no reason to impose additional notice or consent requirements on carriers.

Similarly, there is no basis for requiring purchasing carriers to re-obtain approval to use and disclose CPNI from newly acquired customers.^{14/} First, if customers want to change their vote concerning the new carrier's use of their CPNI, they can do so at any time.^{15/} In addition, when a carrier buys another carrier or substantially all of its assets, the selling carrier must represent to the Commission that it is in compliance with the agency's CPNI rules.^{16/} Once the transaction has been consummated, the new carrier is required to comply with the CPNI notification rules, which, among other things, require a carrier to provide notice of the opt-out process to its customers every two years.^{17/} This requirement ensures that the transferred customers continue to be notified sufficiently of their choices regarding the treatment of their

^{13/} AT&T Wireless Privacy Policy, *available at* <http://www.attws.com/privacy>. Several other carriers also provide their customers with notice that personal information may be disclosed to an acquiring carrier in the event of a business transfer. *See, e.g.,* VoiceStream Wireless T-Mobile Privacy Notice, (“‘personally identifiable’ customer information may be transferred as one of the business assets in the transaction.”), *available at* <http://www.t-mobile.com/info/legal/T-MobilePrivacyNotice.doc>; Qwest Customer Privacy Policy, (“Qwest may . . . decide to sell or transfer parts of [their] business to unaffiliated companies. When this happens, [Qwest] may provide confidential customer information to these companies so that they can offer . . . the same or similar services.”), *available at* <http://www.qwest.com/legal/privacy.html>.

^{14/} *Third Further Notice* ¶ 146.

^{15/} *Id.* at Appendix B, 47 C.F.R. § 64.2008(d)(3)(E). Sections 64.2007, 64.2008, and 64.2009 of the Commission's new CPNI rules, as cited herein, will be effective upon OMB approval. *See Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, As Amended*, 67 Fed. Reg. 59205 (September 20, 2002).

^{16/} *Third Further Notice* at Appendix B, 47 C.F.R. §§ 64.2005-64.2009.

^{17/} *Third Further Notice* at Appendix B, 47 C.F.R. § 64.2008(d)(2).

CPNI. Taken together, these two factors ensure that a customer's privacy rights are adequately protected, without imposing additional and potentially very costly requirements on carriers.

CONCLUSION

For the foregoing reasons, the Commission should clarify that the FBI's letter does not apply to the CPNI of wireless customers roaming overseas, and should explicitly exempt wireless roaming from any foreign storage or access rules it may adopt. In addition, the Commission should confirm that carriers are able to use and disclose CPNI as part of a business transfer.

Respectfully submitted,

AT&T WIRELESS SERVICES, INC.

Howard J. Symons
Sara F. Leibman
Susan S. Ferrel
Mintz, Levin, Cohn, Ferris, Glovsky
and Popeo, P.C.
701 Pennsylvania Avenue, N.W.
Suite 900
Washington, D.C. 20004
(202) 434-7300

Of Counsel

Dated: October 21, 2002

/s/ Douglas I. Brandon

Douglas I. Brandon
Vice President - External Affairs
David P. Wye
Director, Spectrum Policy
1150 Connecticut Avenue, N.W.
Suite 400
Washington, D.C. 20036
(202) 223-9222

CERTIFICATE OF SERVICE

I, Susan S. Ferrel, hereby certify that on this 21st day of October 2002, the foregoing Comments of AT&T Wireless Services, Inc. were filed electronically on the FCC's Electronic Comment Filing System and electronic copies were served via electronic mail to the following:

Marlene H. Dortch
Secretary
Federal Communications Commission
Office of the Secretary
c/o Vistronix, Inc.
236 Massachusetts Avenue, N.E.
Suite 110
Washington, DC 20002

William Maher
Chief
Wireline Competition Bureau
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554
Wmaher@fcc.gov

Jeffrey Carlisle
Senior Deputy Chief
Wireline Competition Bureau
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554
jcarlisl@fcc.gov

Thomas J. Sugrue
Chief
Wireless Telecommunications Bureau
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554
tsugrue@fcc.gov

James D. Schlichting
Deputy Chief
Wireless Telecommunications Bureau
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554
jschlich@fcc.gov

Marcy Greene
Attorney Advisor
Competition Policy Division
Wireline Competition Bureau
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554
mgreene@fcc.gov

Qualex International
Portals II
445 12th Street, S.W. Room CY-B402
Washington, D.C. 20554
qualexint@aol.com

/s/ Susan S. Ferrel
Susan S. Ferrel